ASA 7.1/7.2 ：在 ASA 上允许 SVC 使用分割隧道的配置示例

目录

简介

本文档针对在安全套接字层 (SSL) VPN 客户端 (SVC) 通过隧道连接到 Cisco 自适应安全设备 (ASA) 时如何允许这些 VPN 客户端访问 Internet 提供分步说明。 此配置允许通过 SSL 对公司资源进行 SVC 安全访问，并使用分割隧道提供对 Internet 的非安全访问。

使用同一个接口同时传输安全数据流和非安全数据流的功能称为分割隧道。分割隧道要求您明确指定哪个是安全数据流以及该数据流的目标是什么，这样只有指定的数据流进入隧道，而其余数据流则以未加密形式通过公共网络 (Internet) 进行传输。

先决条件

要求

尝试进行此配置之前，请确保满足以下要求：

- 在所有远程工作站上都有本地管理权限
- 在远程工作站上有 Java 和 Activex 控件
- 端口 443 (SSL) 在连接路径中的任何位置都不受阻止

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 运行软件版本 7.2(2) 的 Cisco 5500 系列自适应安全设备 (ASA)
- 适用于 Windows 1.1.4.179 的 Cisco SSL VPN Client 版本**注意：**从思科软件下载（仅限注册客户）下载SSL VPN客户端包(sslclient-win*.pkg)(仅限注册客户)。 将 SVC 复制到 ASA 的闪存，前者需要下载到远程用户计算机以便建立与 ASA 的 SSL VPN 连接。有关详细信息，请参阅 ASA 配置指南的安装 SVC 软件部分。
- 运行 Windows 2000 Professional SP4 或 Windows XP SP2 的 PC
- Cisco 自适应安全设备管理器 (ASDM) 版本 5.2(2)

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文档约定的更多信息，请参考 Cisco 技术提示约定。

背景信息

SSL VPN 客户端 (SVC) 是一种 VPN 隧道技术，这种技术让远程用户可以利用 IPsec VPN 客户端的优势，而无需网络管理员在远程计算机上安装和配置 IPsec VPN 客户端。SVC 使用远程计算机上已经具有的 SSL 加密以及安全设备的 WebVPN 登录和身份验证。

为建立 SVC 会话，远程用户需要在浏览器中输入安全设备 WebVPN 接口的 IP 地址，浏览器便会连接到该接口并显示 WebVPN 登录屏幕。如果您完成登录并通过身份验证，而且安全设备将您识别为需要 SVC，则会将 SVC 下载到远程计算机。如果安全设备将您识别为可以选择使用 SVC，它会将 SVC 下载到远程计算机，但在窗口中显示一个跳过 SVC 安装的链接。

下载完成后，SVC 将自行安装并配置，随后当连接终止时，SVC 会在远程计算机中保留或卸载自己，具体取决于配置。

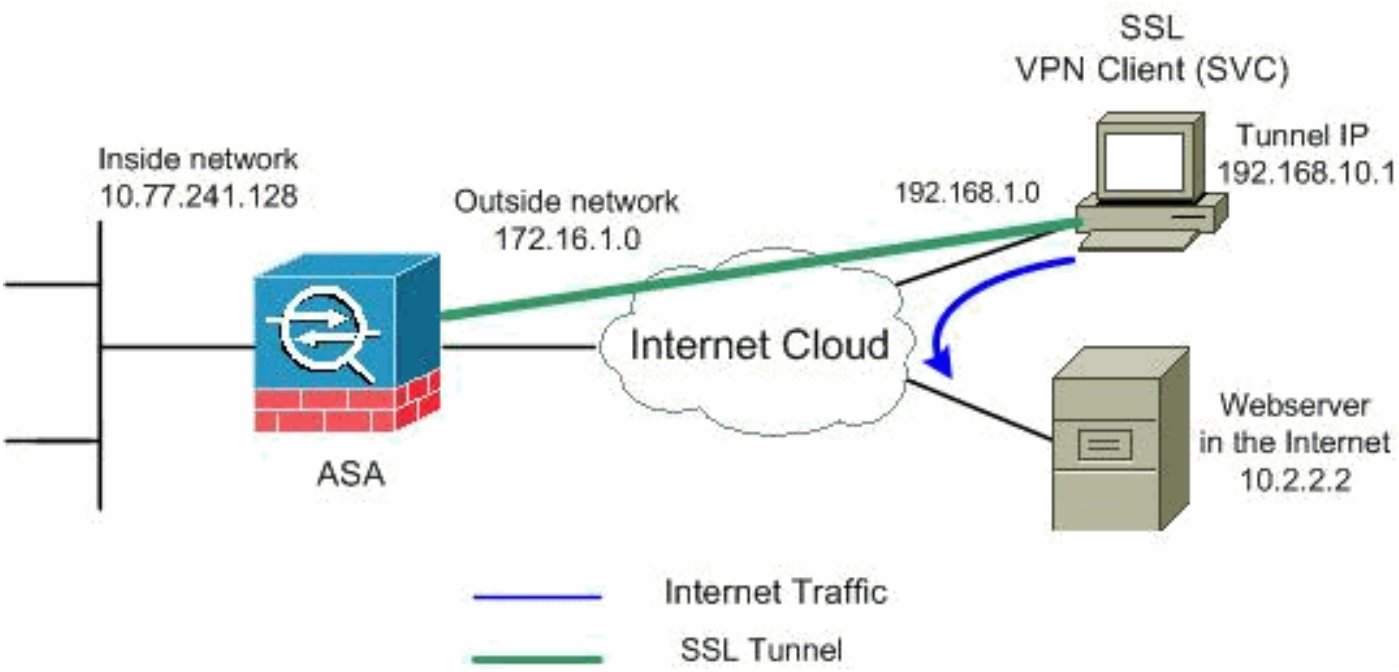
配置

本部分提供有关如何配置本文档所述功能的信息。

注意：要获取有关本部分中所使用命令的更多信息，可使用命令查找工具（仅限已注册客户）。

网络图

本文档使用以下网络设置：

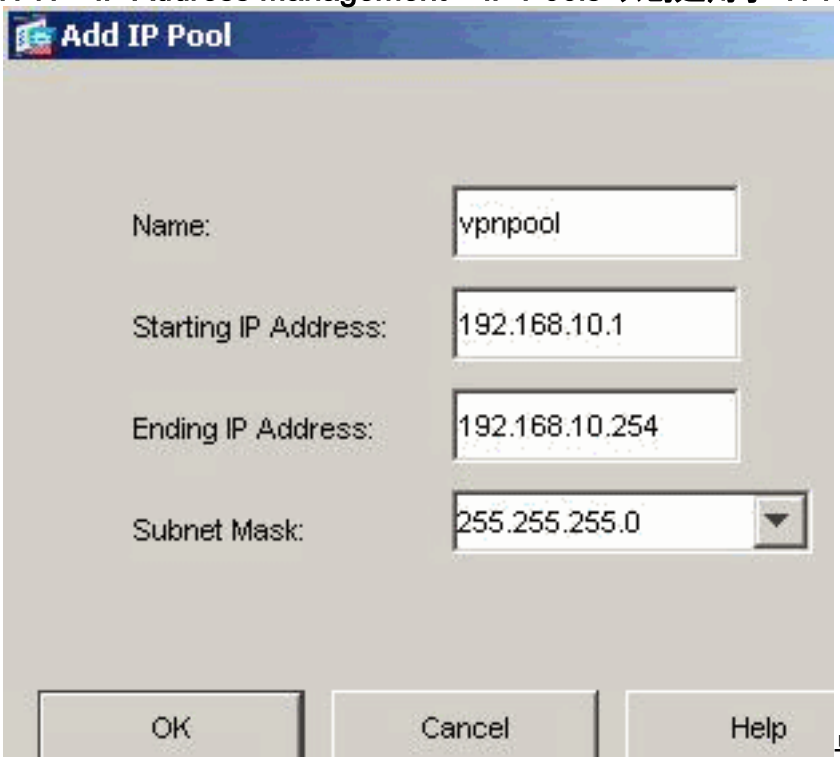


注意：此配置中使用的IP编址方案在Internet上不可合法路由。这些地址是在实验室环境中使用的 RFC 1918 地址。

使用 ASDM 5.2(2) 配置 ASA

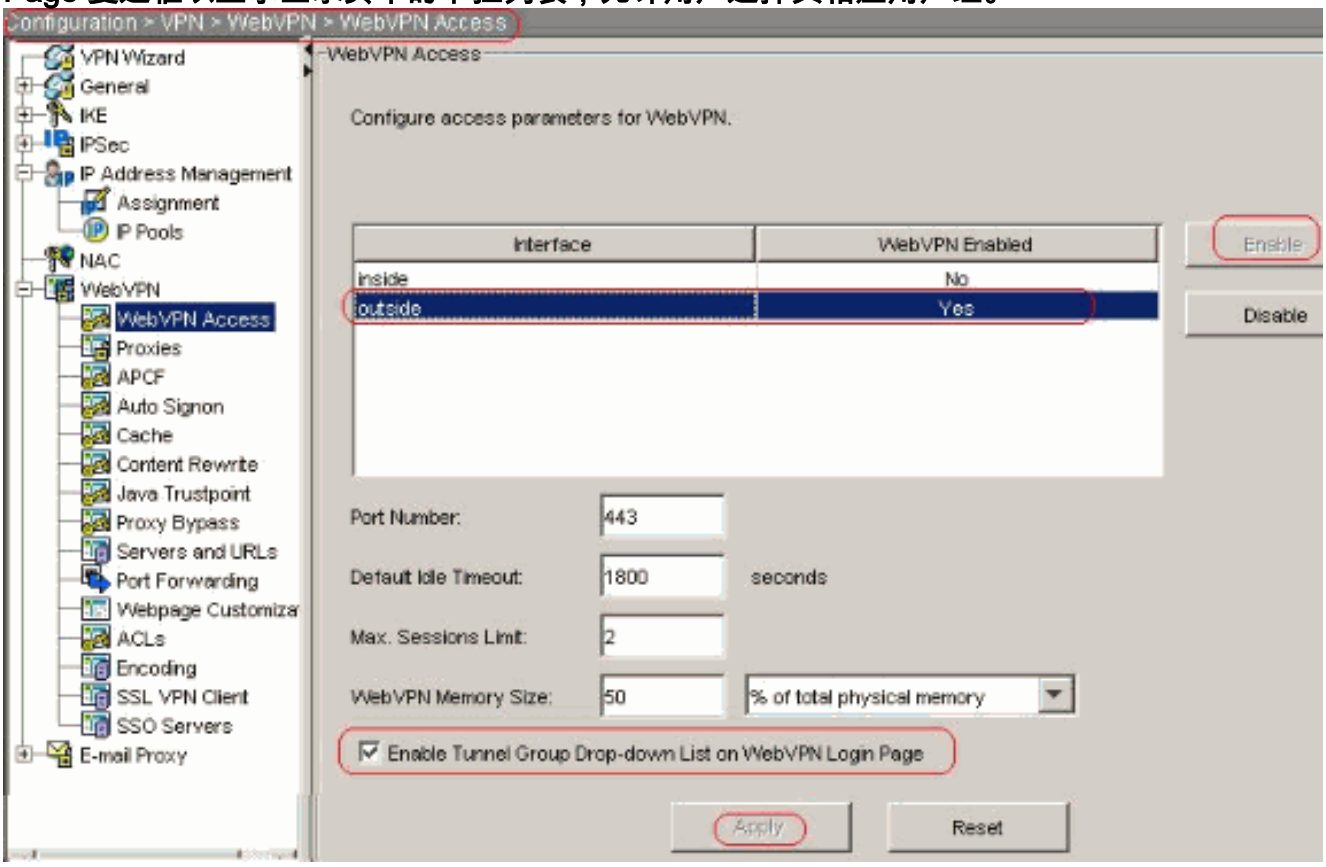
若要在 ASA 上为 SSL VPN 配置分割隧道，请完成下列步骤：

1. 本文档假定基本配置（如接口配置等）已完成并且可以正常工作。**注意**：请参阅允许ASDM的HTTPS访问，以便允许ASDM配置ASA。**注意**：除非更改端口号，否则无法在同一ASA接口上启用WebVPN和ASDM。有关详细信息，请参阅在相同 ASA 接口上同时启用 Webvpn 和 ASDM。
2. 选择 **Configuration > VPN > IP Address Management > IP Pools 以创建用于 VPN 客户端的 IP 地址池：vpnpool。**

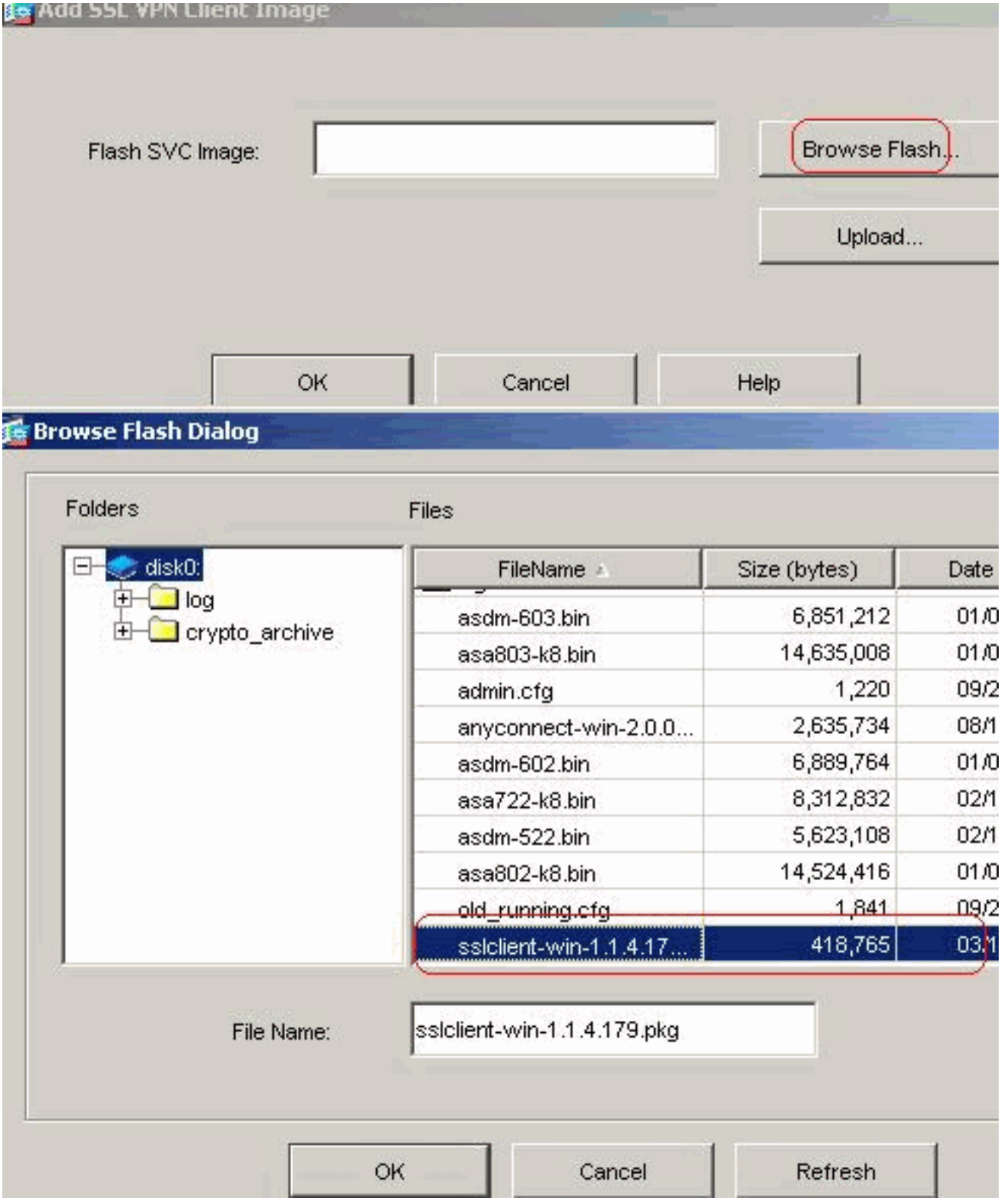


单击 Apply。
3. **启用 WebVPN选择 Configuration > VPN > WebVPN > WebVPN Access，然后用鼠标突出显**

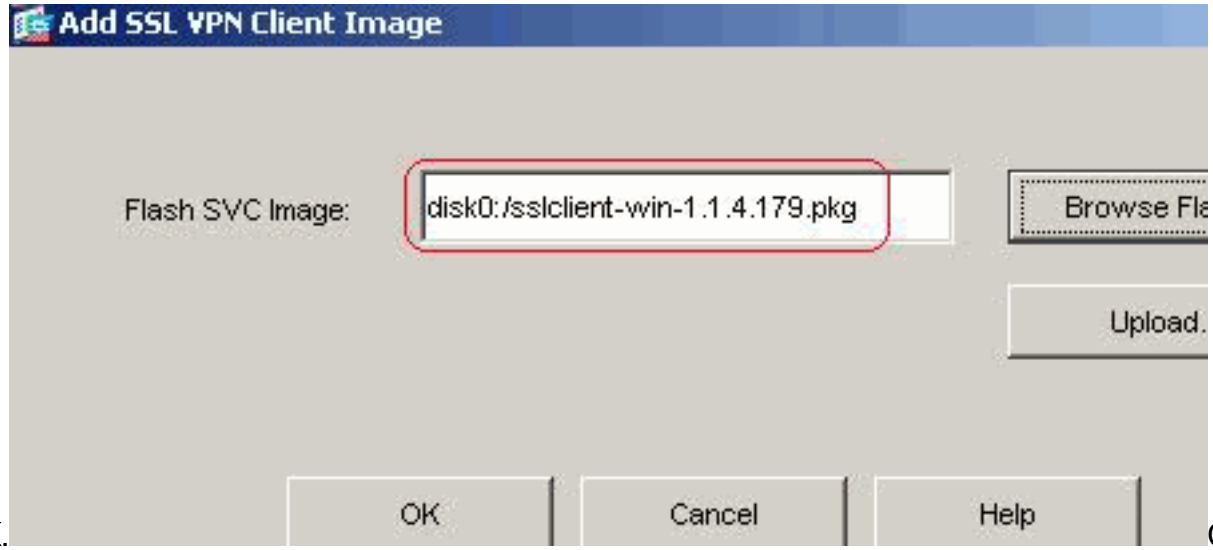
示外部接口并单击“Enable”。选中 Enable Tunnel Group Drop-down List on WebVPN Login Page 复选框以显示登录页中的下拉列表，允许用户选择其相应用户组。



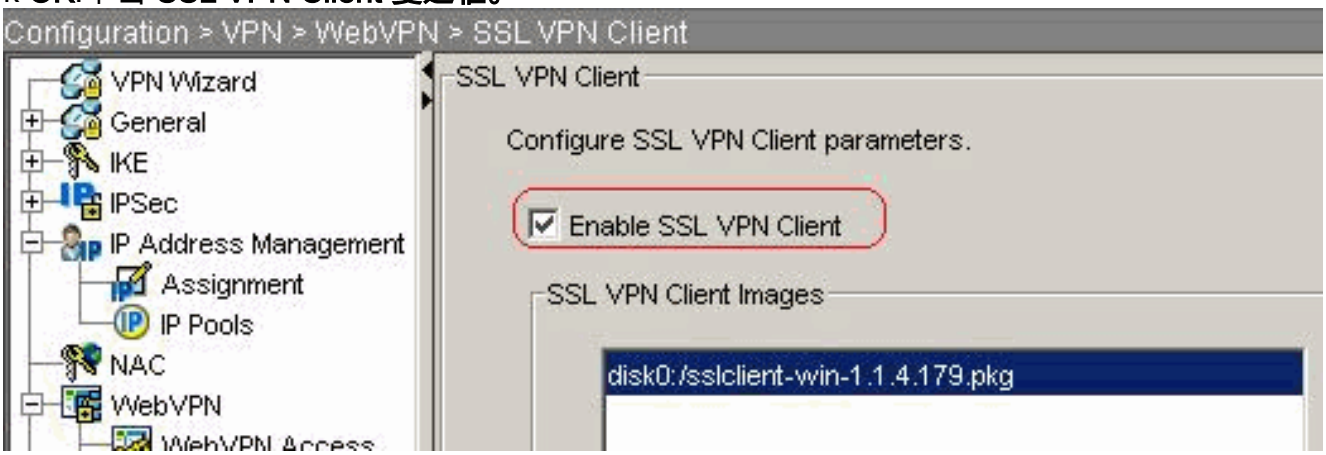
单击 Apply。选择 Configuration > VPN > WebVPN > SSL VPN Client > Add 以便从 ASA 闪存中添加 SSL VPN 客户端映像，如下所示。


Add SSL VPN Client Image
Flash SVC Image:
Browse Flash...
Upload...
OK
Cancel
Help
Browse Flash Dialog
Folders
Files
disk0:
log
crypto_archive
FileName
Size (bytes)
Date
asdm-603.bin
6,851,212
01/0
asa803-k8.bin
14,635,008
01/0
admin.cfg
1,220
09/2
anyconnect-win-2.0.0...
2,635,734
08/1
asdm-602.bin
6,889,764
01/0
asa722-k8.bin
8,312,832
02/1
asdm-522.bin
5,623,108
02/1
asa802-k8.bin
14,524,416
01/0
old_running.cfg
1,841
09/2
sslclient-win-1.1.4.17...
418,765
03/1
File Name:
sslclient-win-1.1.4.179.pkg
OK
Cancel
Refresh

Click

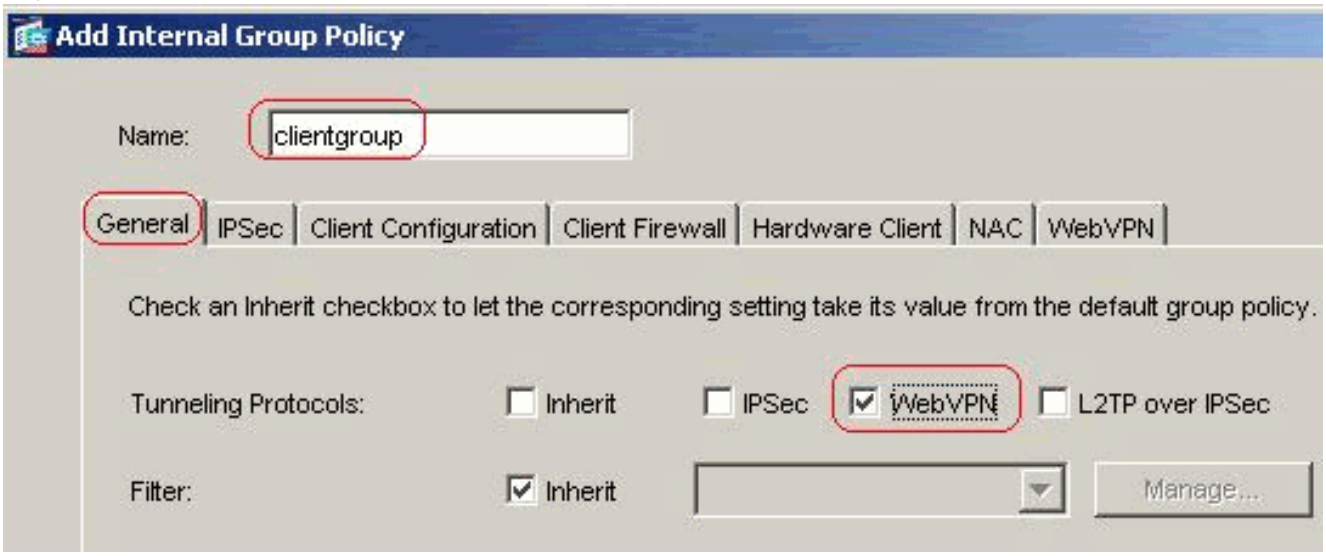


OK. Click OK.单击 SSL VPN Client 复选框。

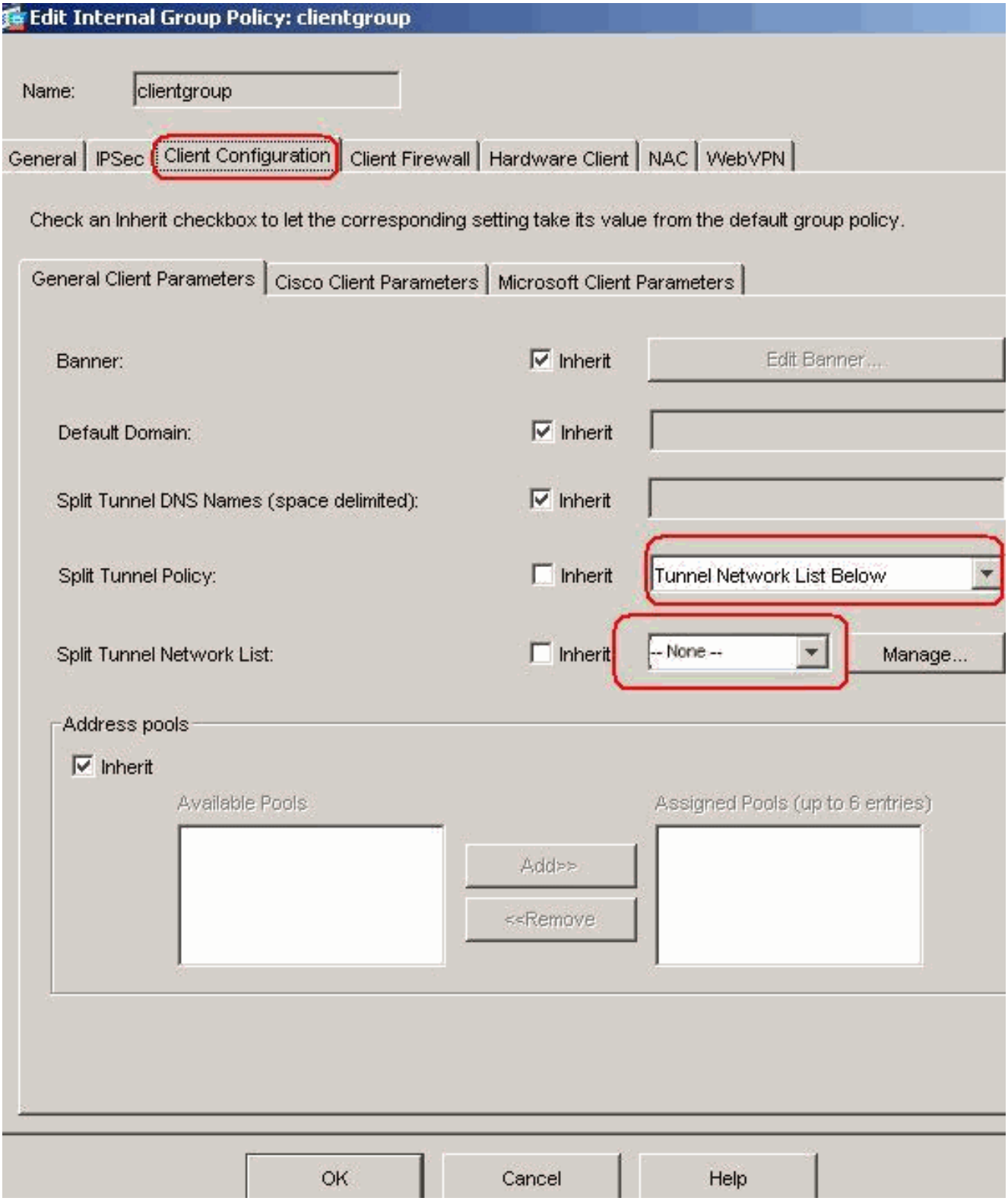


单击 Apply。等效 CLI 配置：

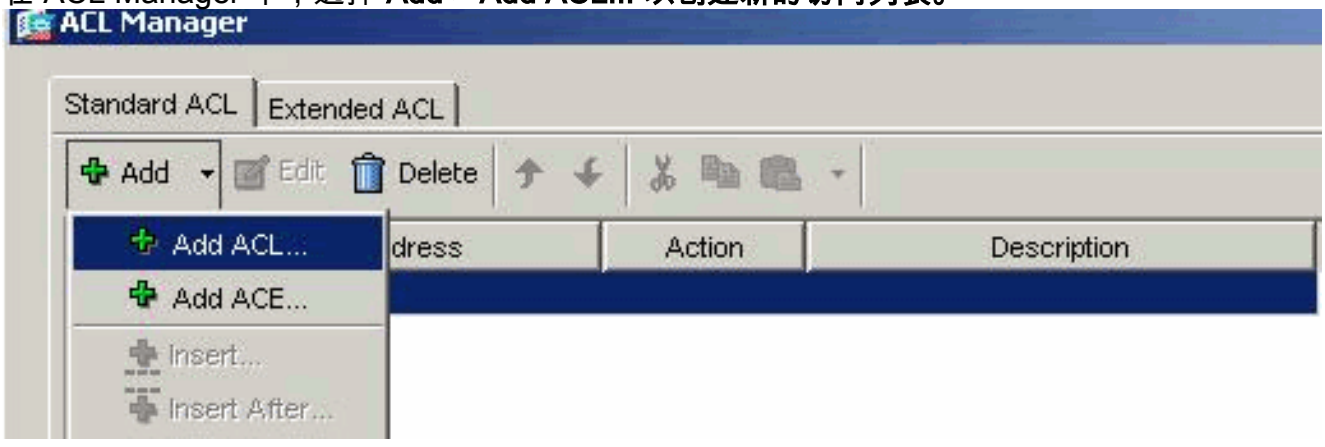
4. 配置组策略选择 Configuration > VPN > General > Group Policy > Add (Internal Group Policy) 以创建内部组策略 clientgroup。在 General 下选中“WebVPN”复选框，以启用 WebVPN 作为隧道协议。



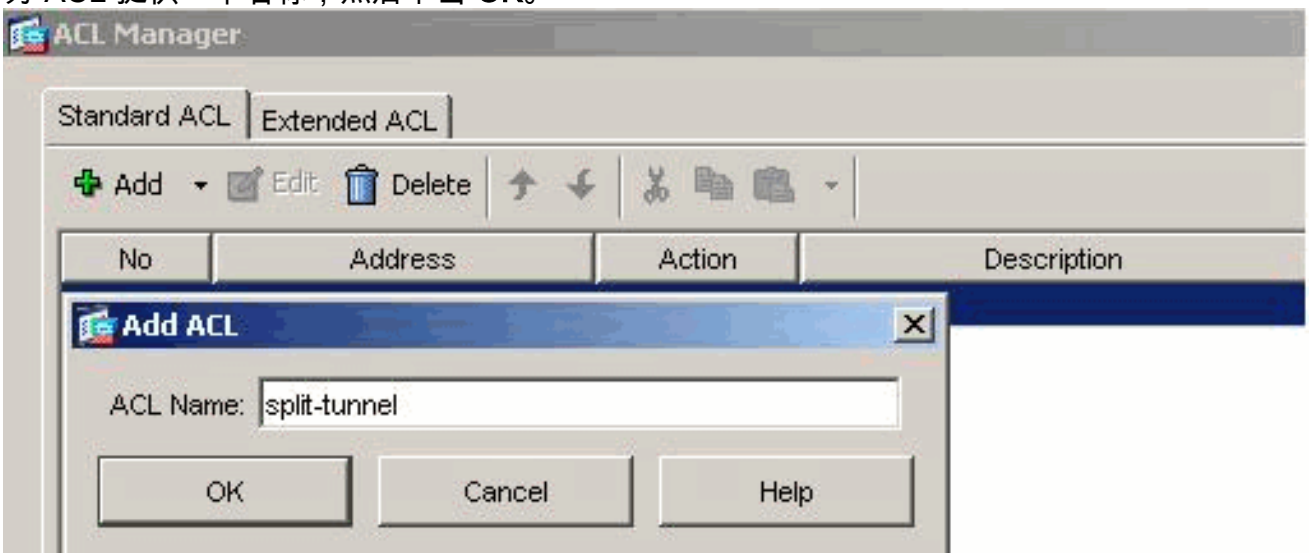
在 Client Configuration > General Client Parameters 选项卡中，取消选中“Inherit box for Split Tunnel Policy”，并从下拉列表中选择“Tunnel Network List Below”。取消选中 Split Tunnel Network List 所对应的 Inherit 框，然后单击 Manage 启动 ACL Manager。



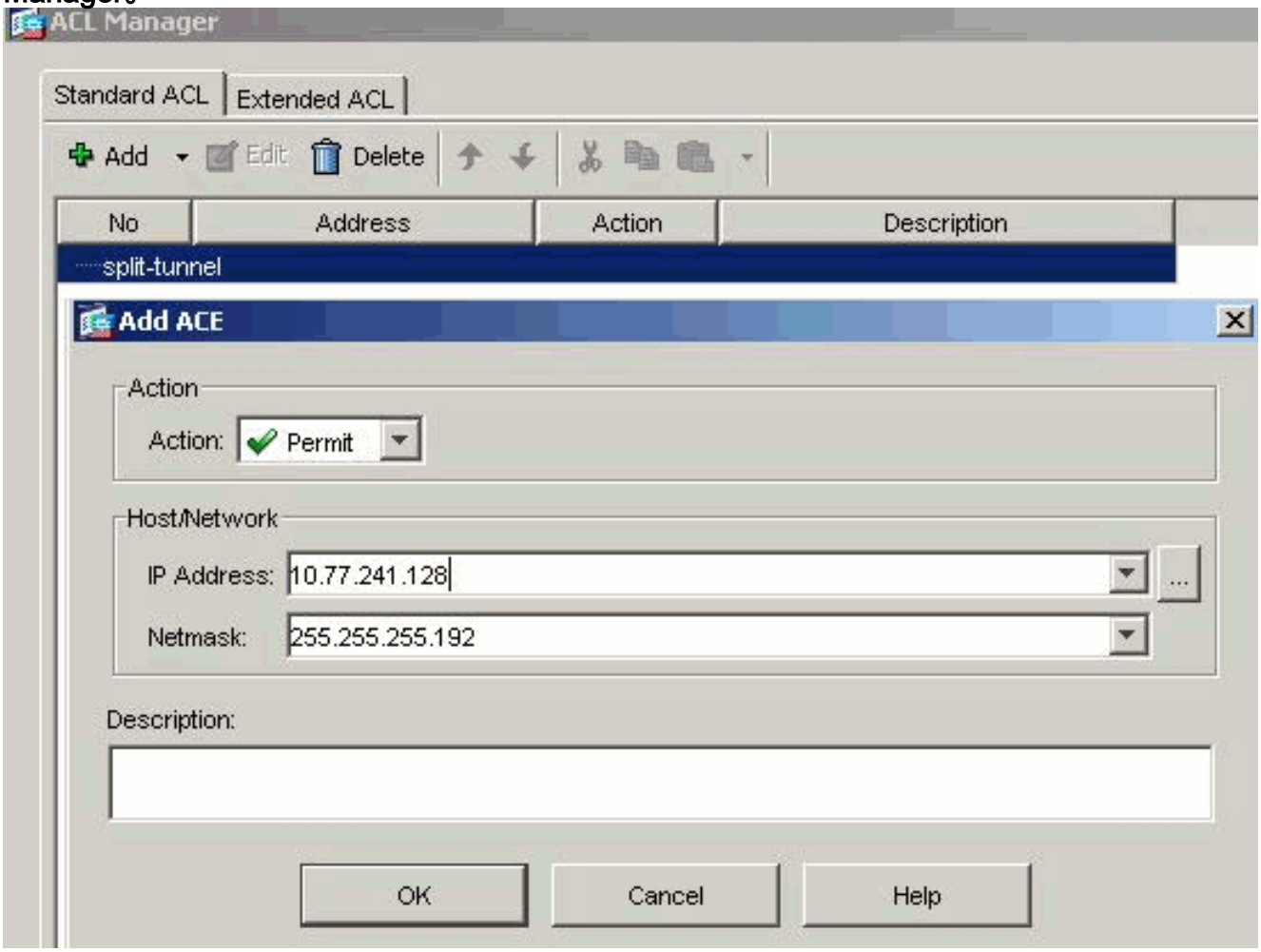
在 ACL Manager 中，选择 **Add > Add ACL... 以创建新的访问列表。**



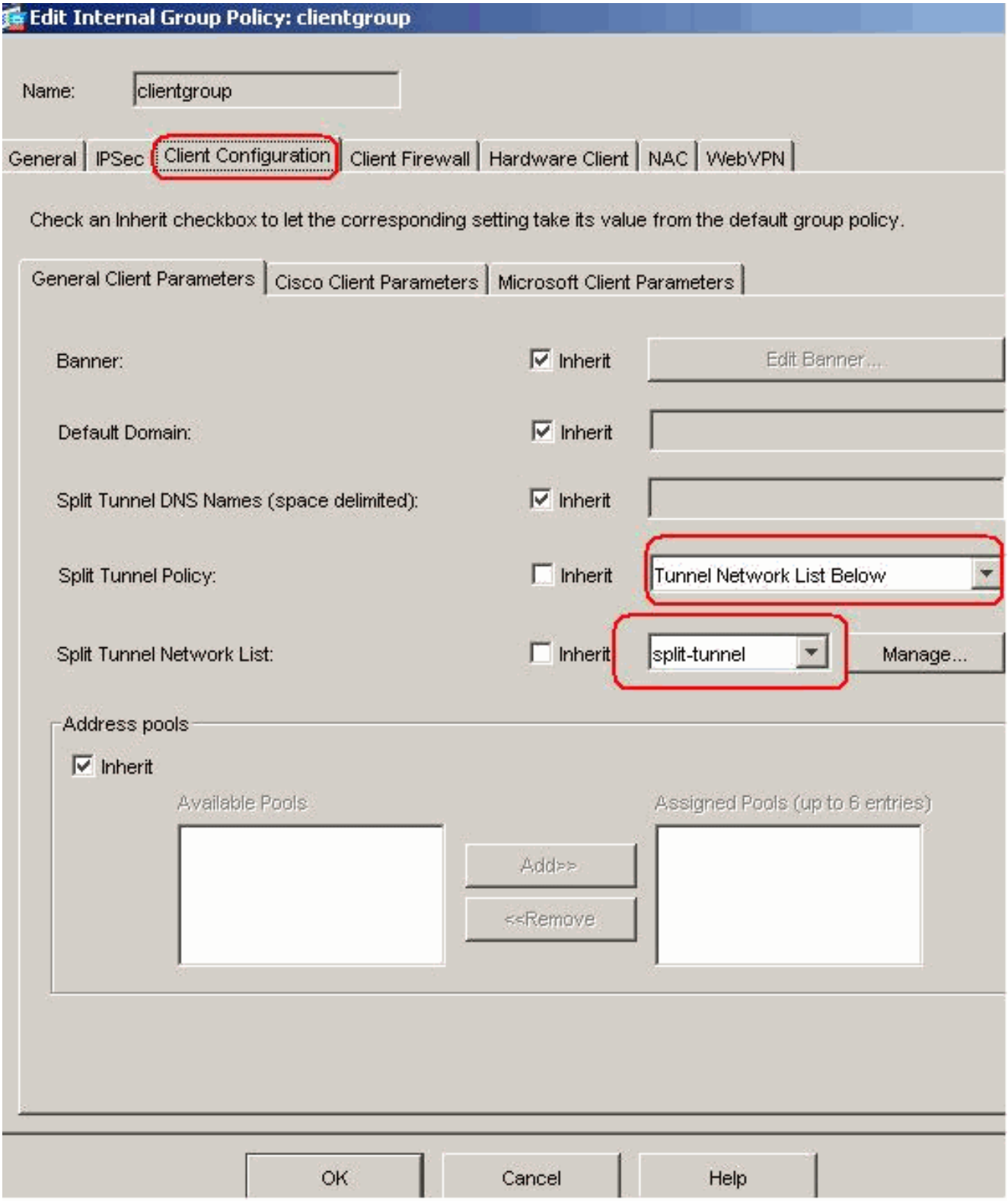
为 ACL 提供一个名称，然后单击 **OK**。



创建 ACL 名称后，选择 **Add > Add ACE 以添加访问控制项 (ACE)。**定义与 ASA 后的 LAN 对应的 ACE。在这种情况下，网络为 10.77.241.128/26，选择 **Permit**。单击 **OK 以退出 ACL Manager。**

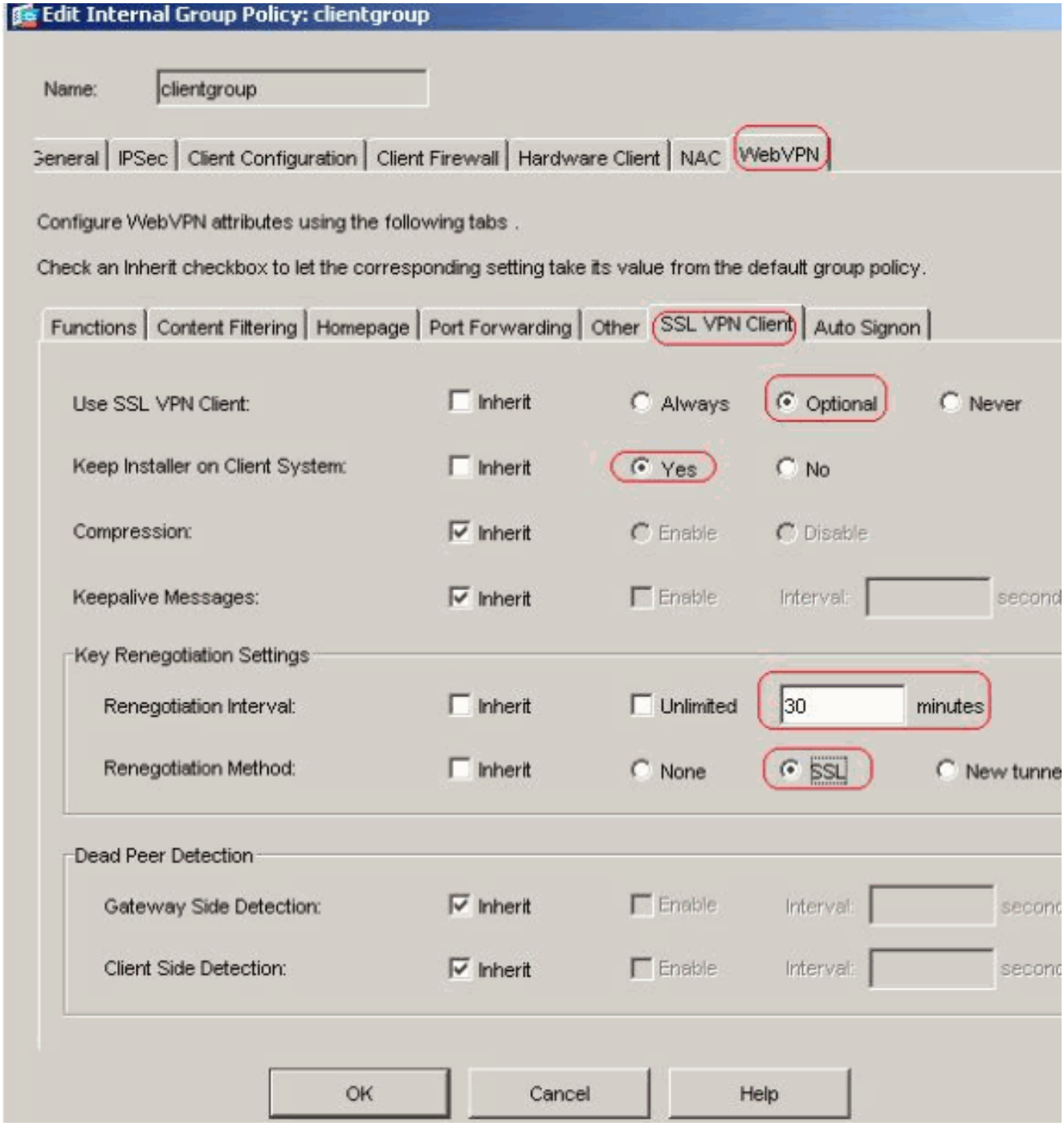


确保在 Split Tunnel Network List 中选择刚刚创建的 ACL。单击 **OK 以返回组策略配置。**

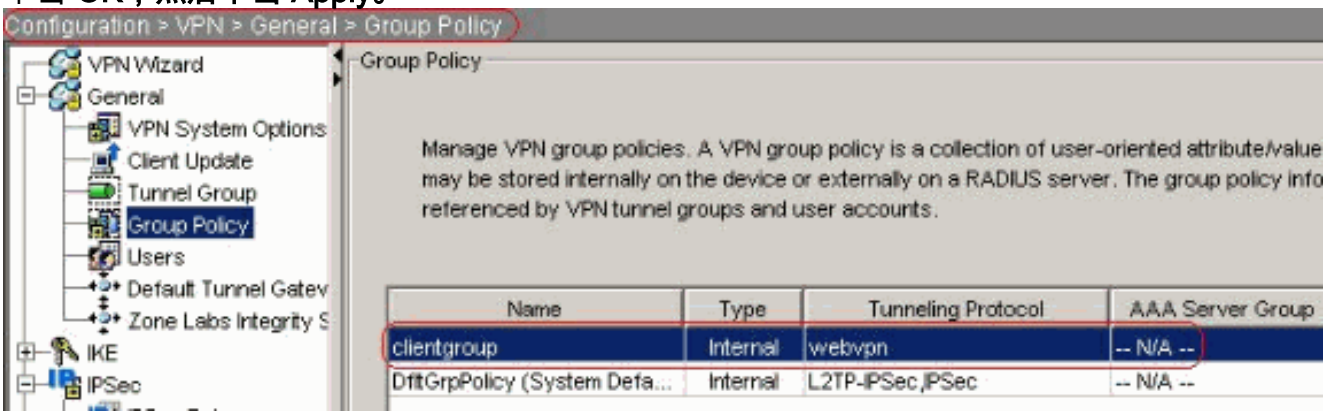


在主页上，单击 **Apply，然后单击“Send”（如果需要），将命令发送到 ASA。**对于“Use SSL VPN Client”选项，取消选中 **Inherit 复选框，然后单击“Optional”单选按钮。**此选项允许远程客户端选择是否单击 **WebVPN > SSLVPN Client 选项卡和选择下列选项：**选择“Do not”将下载 SVC。Always 选择确保在每个 SSL VPN 连接期间将 SVC 下载到远程工作站。对于 Keep Installer on Client System 选项，取消选中 **Inherit 复选框，然后单击 Yes 单选按钮。**通过此操作，SVC 软件可保留在客户端计算机上；因此，不必在每次进行连接时都要求 ASA 将 SVC 软件下载到客户端。对于经常访问企业网络的远程用户而言，此选项是一个很好的选择。对于 Renegotiation Interval 选项，取消选中 **Inherit 框，取消选中 Unlimited 复选框，然后输入重新生成密钥之前经过的分钟数。**如果对密钥的有效时间长度设置限制，可以增强安全性。对于 Renegotiation Method 选项，取消选中 **Inherit 复选框，然后单击 SSL 单选按钮。**重新协商可以使用当前的 SSL 隧道或为重新协商显式创建的新隧道。此时 SSL VPN Client 属性的配置应

如下图所示
：



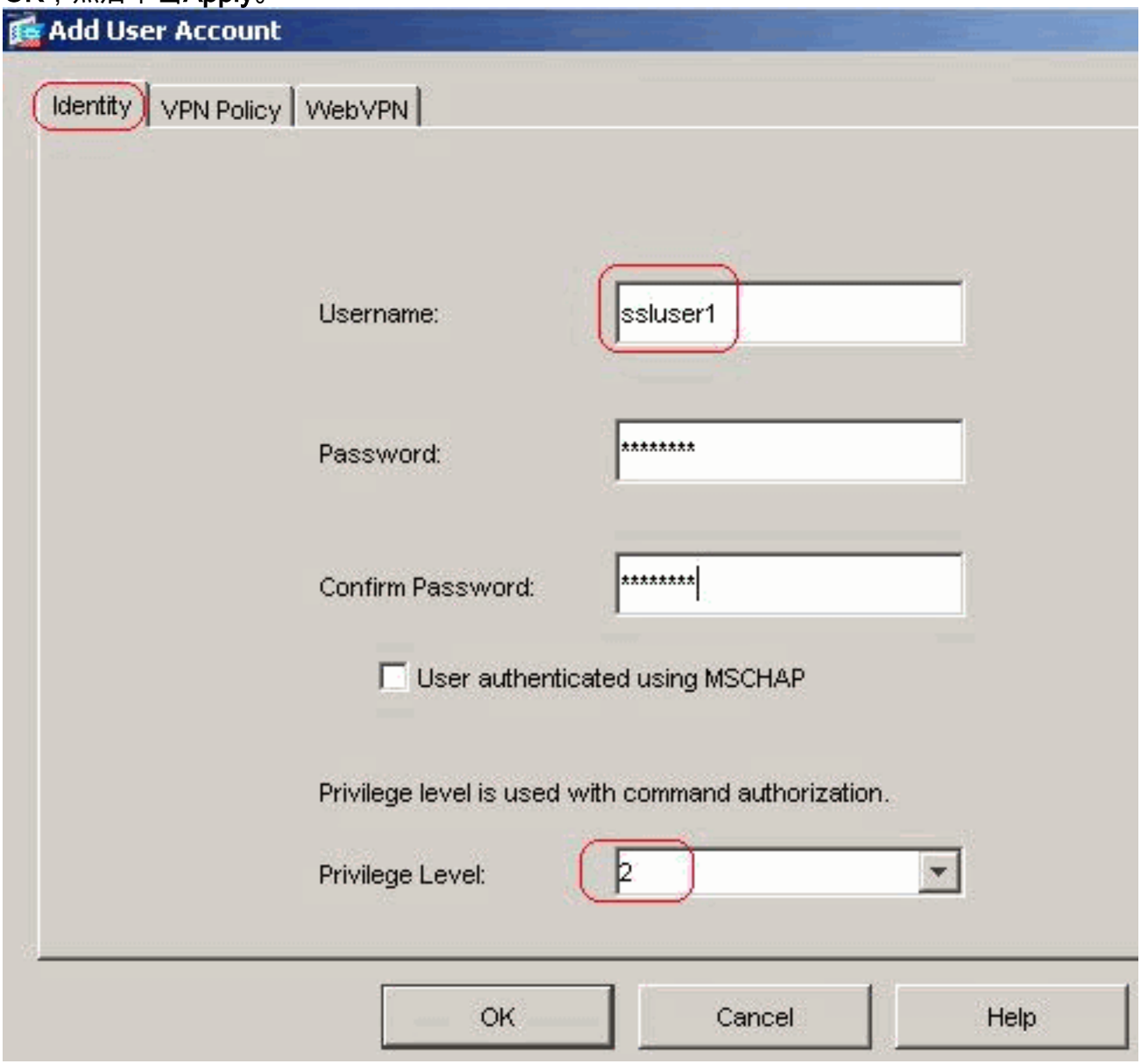
单击 **OK，然后单击 Apply。**



等效 CLI 配置：

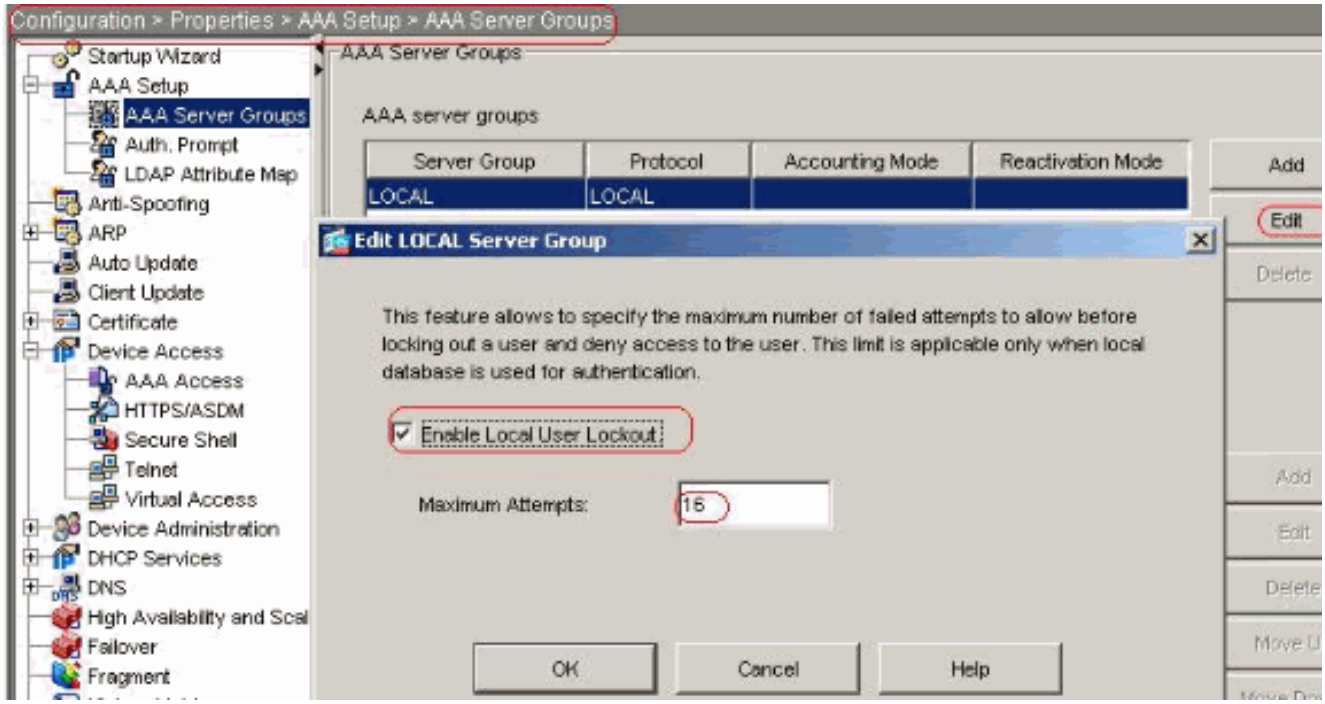
5. 选择**Configuration > VPN > General > Users > Add，以便创建新的用户帐户ssluser1。单击**

OK，然后单击Apply。



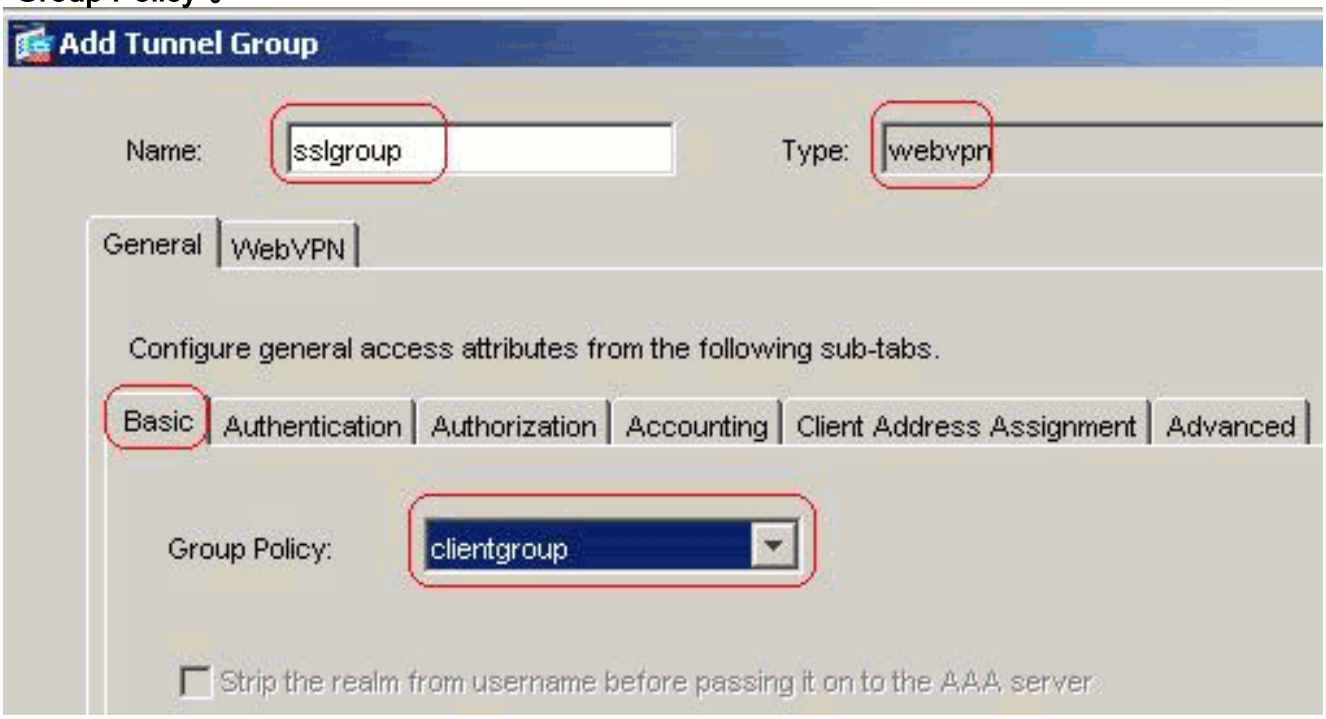
等效 CLI 配置：

6. 选择 Configuration > Properties > AAA Setup > AAA Servers Groups > Edit 以修改默认服务器组 LOCAL，选中“Enable Local User Lockout”复选框并将最大尝试次数值设置为 16。

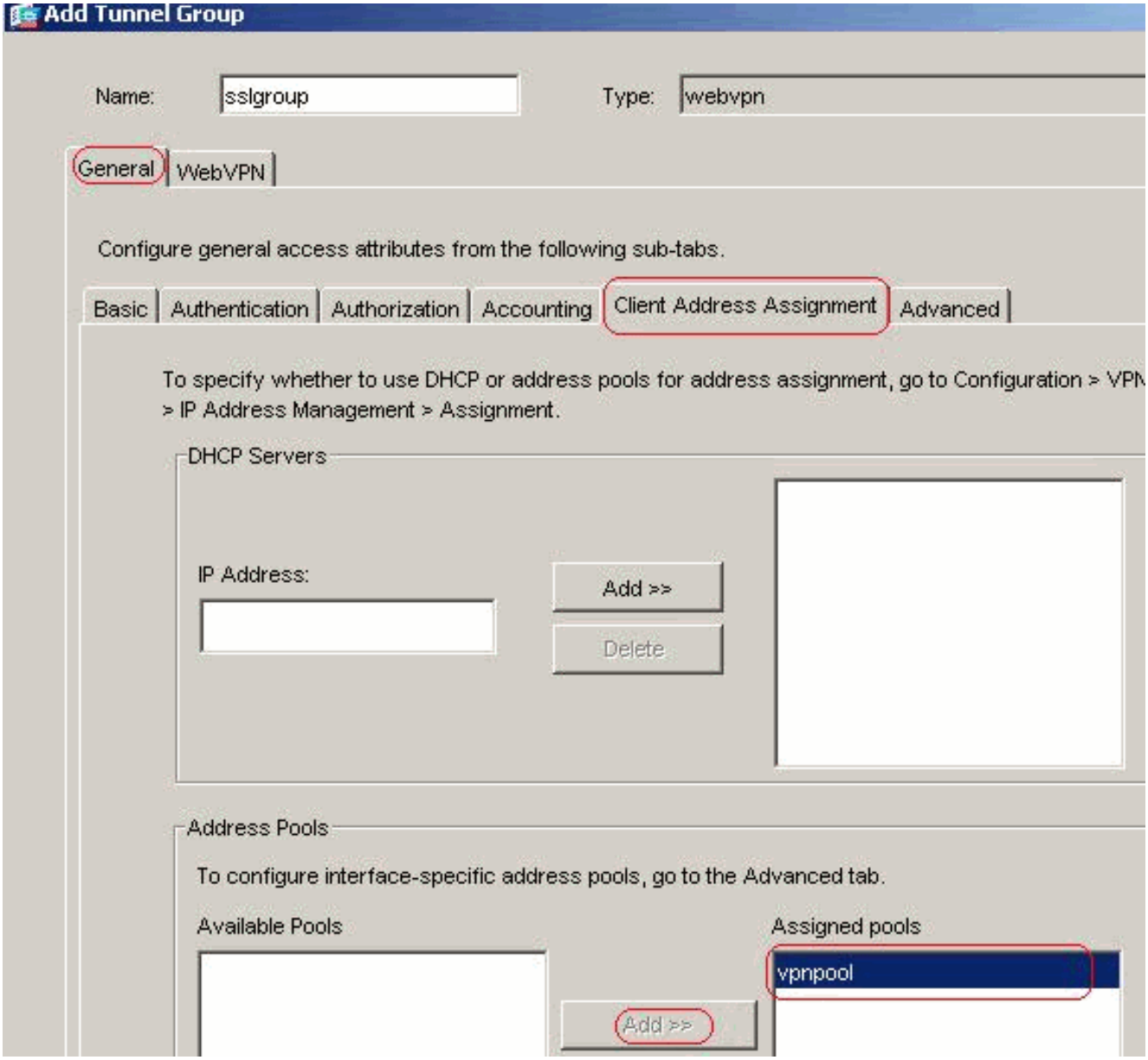


等效 CLI 配置：

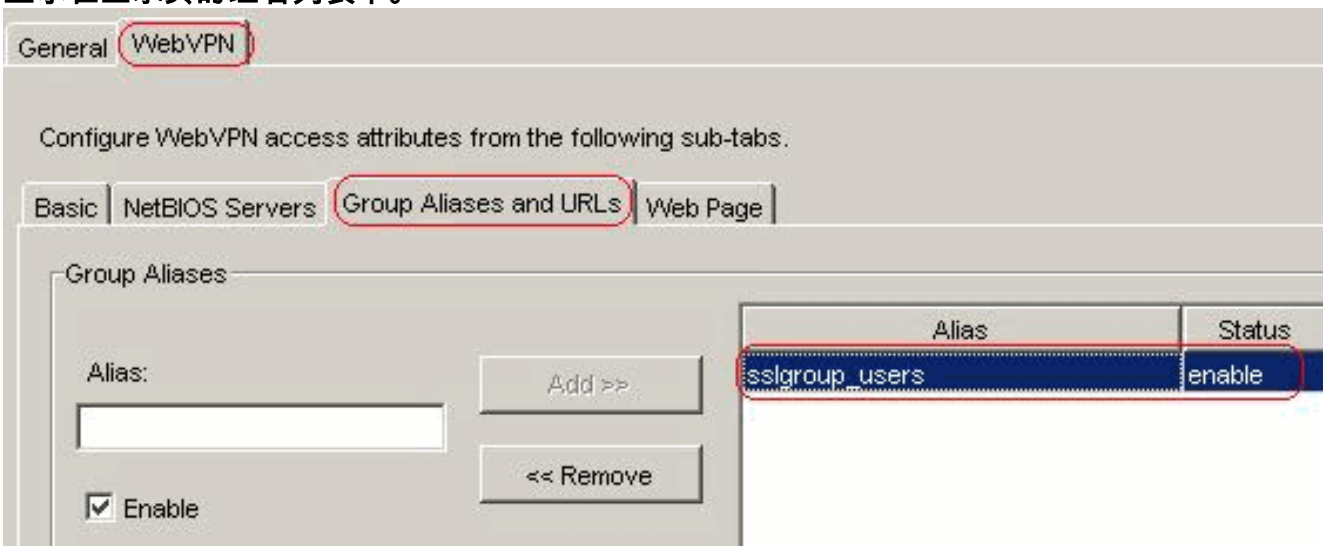
7. **配置隧道组**选择 **Configuration > VPN > General > Tunnel Group > Add (WebVPN access) 以创建新隧道组 sslgroup。**在 **General > Basic 选项卡中，从下拉列表中选择 clientgroup 作为“Group Policy”。**



在 General > Client Address Assignment 选项卡中的“Address Pools”下，单击“Add >>”以分配可用地址池 vpnpool。

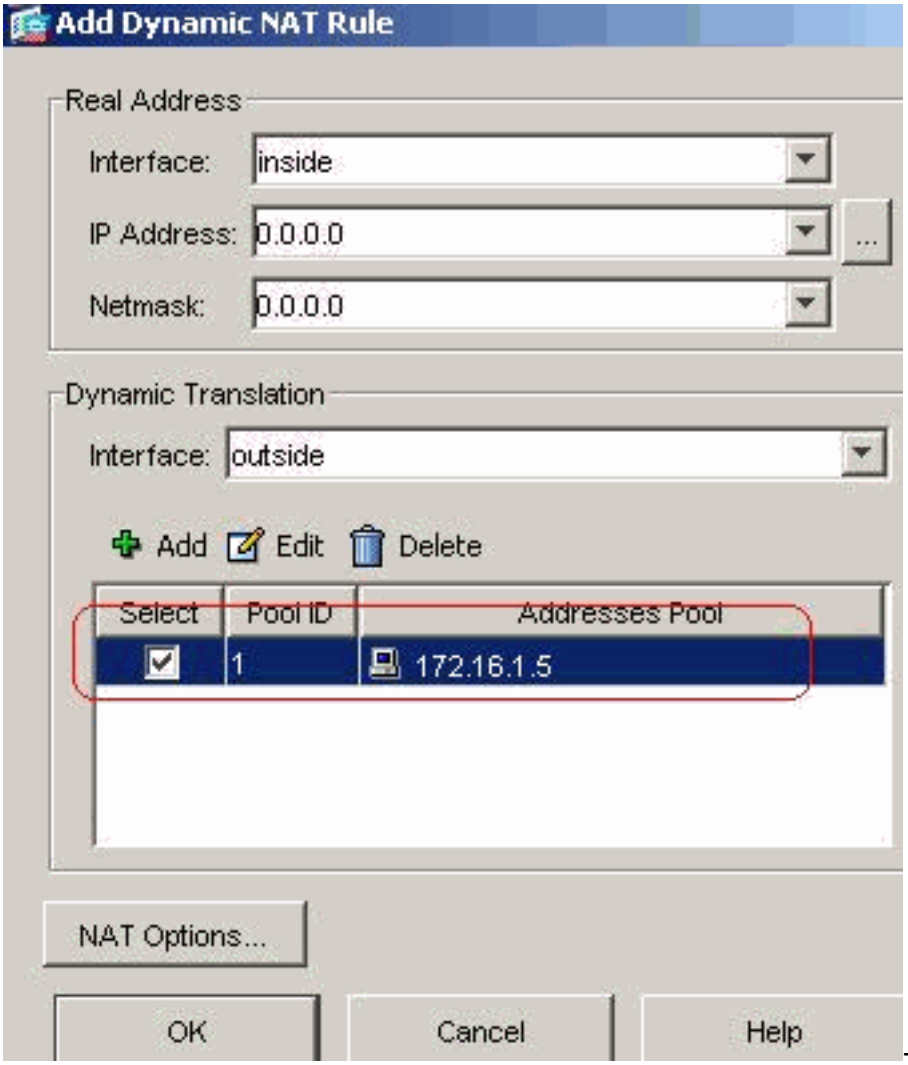


在 WebVPN > Group Aliases and URLs 选项卡中，在参数框中键入别名并单击“Add >>”使其显示在登录页的组名列表中。



单击 OK，然后单击 Apply。等效 CLI 配置：

8. 配置 NAT对于来自可转换为外部 IP 地址 172.16.1.5 的内部网络的数据流，选择 Configuration > NAT > Add > Add Dynamic NAT Rule。



单击 OK，然后在主页中单击“Apply”。等效 CLI 配置：

9. 为从内部网络到VPN客户端的返回流量配置nat-exemption。

```
ciscoasa(config)#access-list nonat permit ip 10.77.241.0 192.168.10.0
ciscoasa(config)#access-list nonat permit ip 192.168.10.0 10.77.241.0
ciscoasa(config)#nat (inside) 0 access-list nonat
```

使用 CLI 配置 ASA 7.2(2)

Cisco ASA 7.2(2)

```
ciscoasa#show running-config
: Saved
:
ASA Version 7.2(2)
!
hostname ciscoasa
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface Ethernet0/0
 nameif inside
 security-level 100
 ip address 10.77.241.142 255.255.255.192
!
interface Ethernet0/1
 nameif outside
 security-level 0
```

```
 ip address 172.16.1.1 255.255.255.0
!
interface Ethernet0/2
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Ethernet0/3
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Management0/0
 shutdown
 no nameif
 no security-level
 no ip address
!
passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive

access-list split-tunnel standard permit 10.77.241.128
255.255.255.192
!--- ACL for Split Tunnel network list for encryption.
access-list nonat permit ip 10.77.241.0 192.168.10.0
access-list nonat permit ip 192.168.10.0 10.77.241.0 !--
- ACL to define the traffic to be exempted from NAT.
pager lines 24 mtu inside 1500 mtu outside 1500 ip local
pool vpnpool 192.168.10.1-192.168.10.254

!--- The address pool for the SSL VPN Clients no
failover icmp unreachable rate-limit 1 burst-size 1 asdm
image disk0:/asdm-522.bin no asdm history enable arp
timeout 14400 global (outside) 1 172.16.1.5

!--- The global address for Internet access used by VPN
Clients. !--- Note: Uses an RFC 1918 range for lab
setup. !--- Apply an address from your public range
provided by your ISP. nat (inside) 0 access-list nonat
!--- The traffic permitted in "nonat" ACL is exempted
from NAT. nat (inside) 1 0.0.0.0 0.0.0.0


access-group 100 in interface outside
route outside 0.0.0.0 0.0.0.0 172.16.1.2 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00
icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp
0:05:00 mgcp-pat 0:05:0
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00
sip-disconnect 0:02:
timeout uauth 0:05:00 absolute
group-policy clientgroup internal

!--- Create an internal group policy "clientgroup".
group-policy clientgroup attributes
 vpn-tunnel-protocol webvpn

!--- Enable webvpn as tunneling protocol. split-tunnel-
policy tunnelspecified
 split-tunnel-network-list value split-tunnel
```

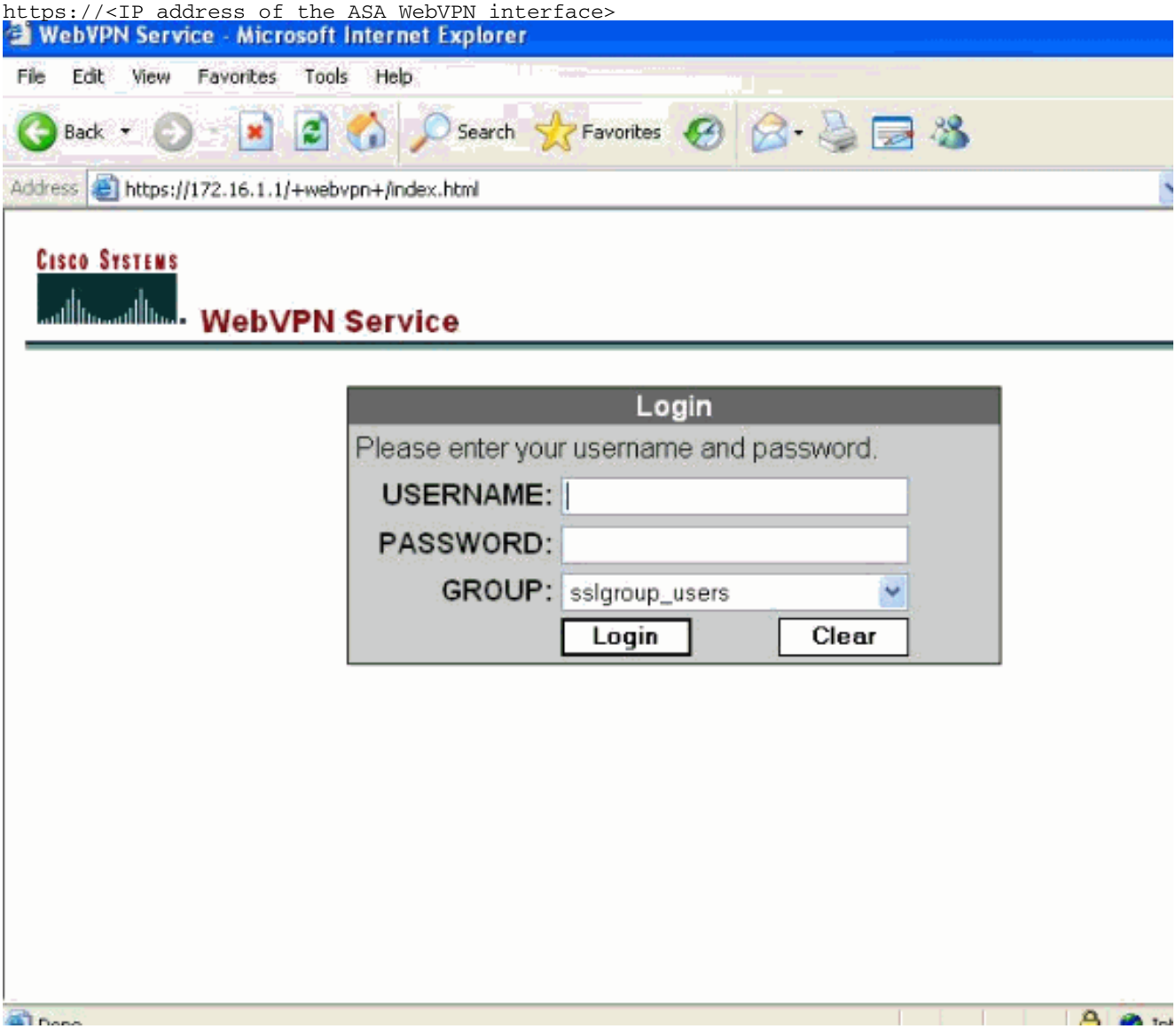
```
!--- Encrypt the traffic specified in the split tunnel
ACL only. webvpn
  svc required

!--- Activate the SVC under webvpn mode. svc keep-
installer installed

!--- When the security appliance and the SVC perform a
rekey, !--- they renegotiate the crypto keys and
initialization vectors, !--- and increase the security
of the connection. svc rekey time 30

!--- Command that specifies the number of minutes !---
from the start of the session until the rekey takes
place, !--- from 1 to 10080 (1 week).  svc rekey method
ssl

!--- Command that specifies that SSL renegotiation !---
takes place during SVC rekey. username ssluser1 password
ZRhW85jZqEaVd5P. encrypted

!--- Create an user account "ssluser1". aaa local
authentication attempts max-fail 16

!--- Enable the AAA local authentication. http server
enable http 0.0.0.0 0.0.0.0 inside no snmp-server
location no snmp-server contact snmp-server enable traps
snmp authentication linkup linkdown coldstart tunnel-
group sslgroup type webvpn

!--- Create a tunnel group "sslgroup" with type as
WebVPN. tunnel-group sslgroup general-attributes
 address-pool vpnpool

!--- Associate the address pool vpnpool created.
default-group-policy clientgroup

!--- Associate the group policy "clientgroup" created.
tunnel-group sslgroup webvpn-attributes

 group-alias sslgroup_users enable

!--- Configure the group alias as sslgroup-users. telnet
timeout 5 ssh timeout 5 console timeout 0 ! class-map
inspection_default match default-inspection-traffic ! !
policy-map type inspect dns preset_dns_map parameters
message-length maximum 512 policy-map global_policy
class inspection_default inspect dns preset_dns_map
inspect ftp inspect h323 h225 inspect h323 ras inspect
netbios inspect rsh inspect rtsp inspect skinny inspect
esmtp inspect sqlnet inspect sunrpc inspect tftp inspect
sip inspect xdmcp ! service-policy global_policy global
webvpn
 enable outside

!--- Enable WebVPN on the outside interface. svc image
disk0:/sslclient-win-1.1.4.179.pkg 1

!--- Assign an order to the SVC image. svc enable

!--- Enable the security appliance to download !--- SVC
images to remote computers. tunnel-group-list enable
```

```
!--- Enable the display of the tunnel-group list !--- on
the WebVPN Login page. prompt hostname context
Cryptochecksum:d41d8cd98f00b204e9800998ecf8427e : end
ciscoasa#
```

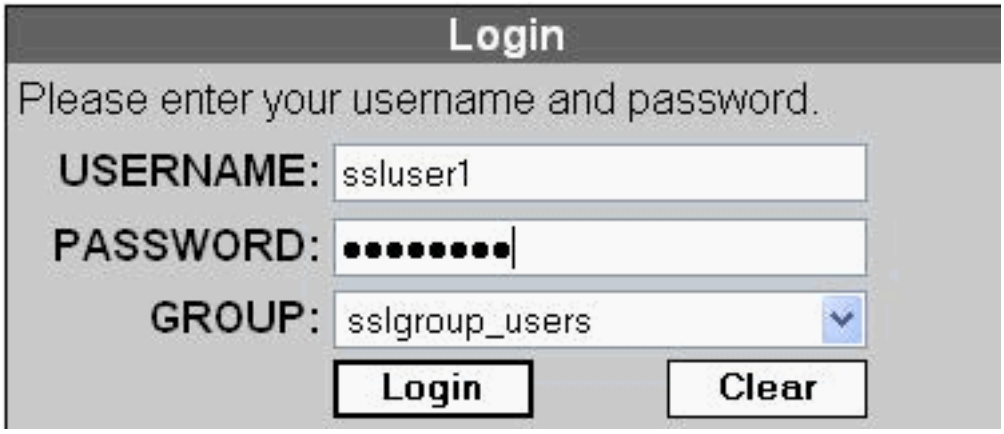
使用 SVC 建立 SSL VPN 连接

要建立与 ASA 的 SSL VPN 连接，请执行以下步骤。

1. 按如下所示格式在 Web 浏览器中键入 ASA WebVPN 接口的 URL 或 IP 地址。
   `https://url`
   或者
   `https://<IP address of the ASA WebVPN interface>`



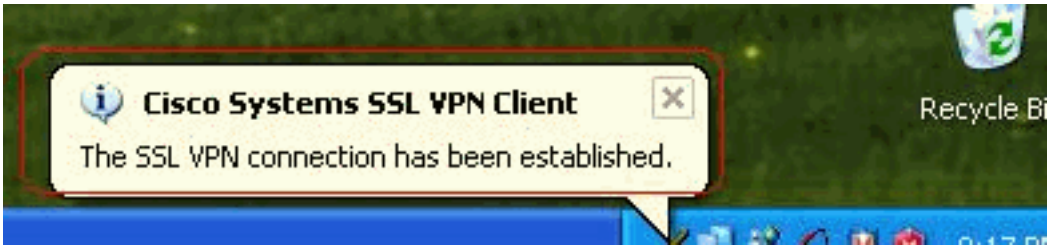
2. 输入用户名和口令，然后从下拉列表中选择相应的组，如下所示。



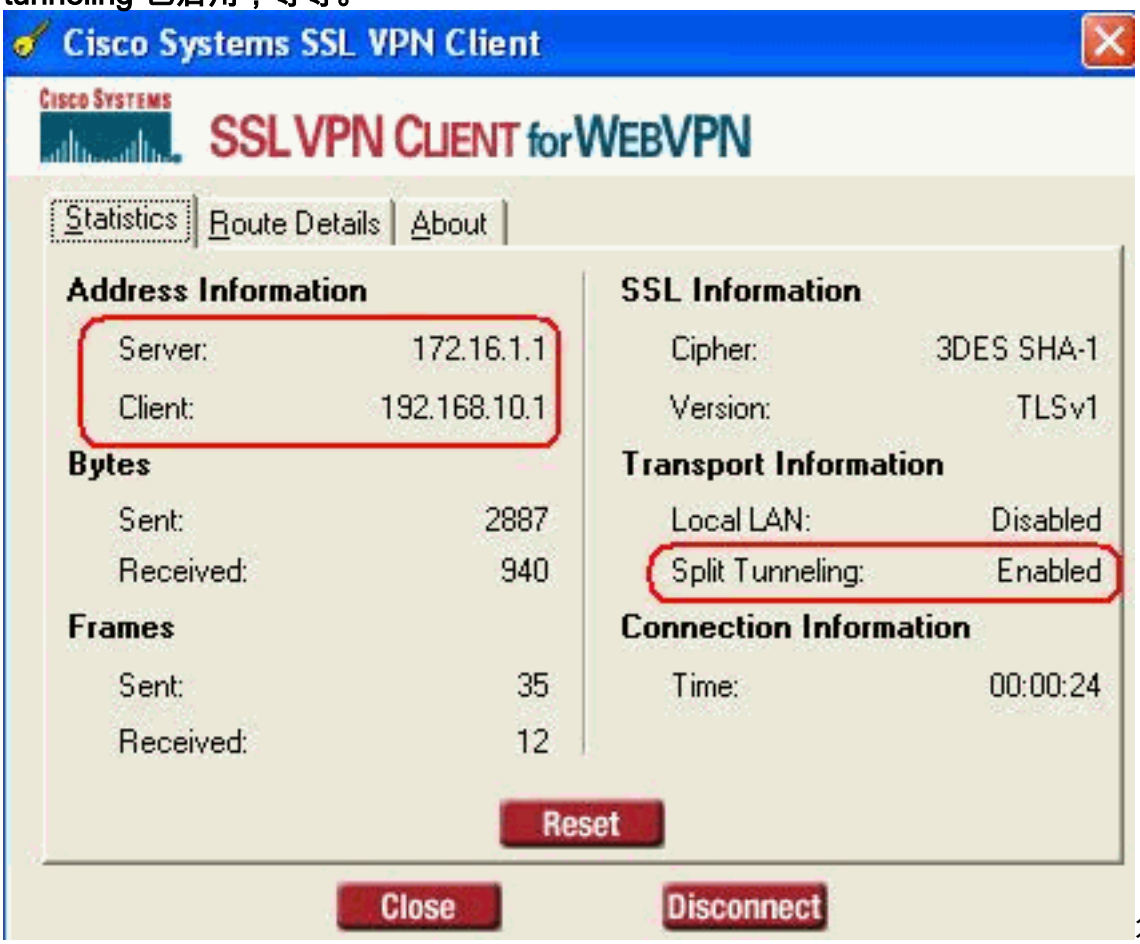
3. 下载 SVC 之前，必须在计算机上安装 ActiveX 软件。

4. 在建立 SSL VPN 连接之前，会显示以下窗口。

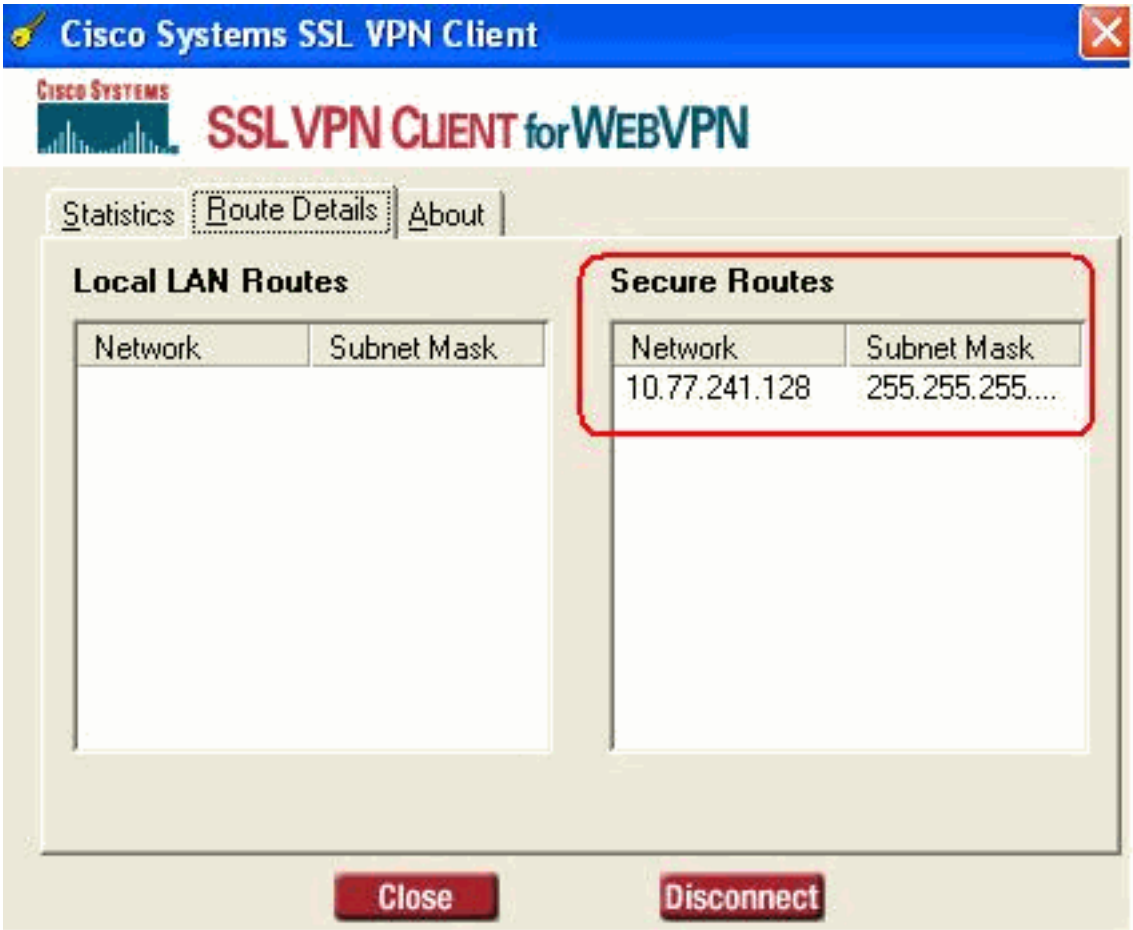
5. 建立连接后，便会显示以下窗口。



6. 单击计算机任务栏中出现的黄色钥匙图标。此时显示以下窗口，其中包含有关 SSL 连接的信息。例如，**192.168.10.1 是分配给客户端的 IP 地址，服务器 IP 地址为 172.16.1.1，“Split tunneling”已启用，等等。**



您还可以检查将由 SSL 进行加密的安全网络，通过 ASA 中配置的分割隧道访问列表可下载网络列表。在本例中，SSL VPN 客户端可以安全访问 10.77.241.128/24，而所有其他数据流不会加密，也不会通过隧道发送。



验证

使用本部分可确认配置能否正常运行。

命令输出解释程序（仅限注册用户）(OIT) 支持某些 show 命令。使用 OIT 可查看对 show 命令输出的分析。

- **show webvpn svc — 显示存储在 ASA 闪存中的 SVC 映像。**

```
ciscoasa#show webvpn svc
1. disk0:/sslclient-win-1.1.4.179.pkg 1
  CISCO STC win2k+ 1.0.0
  1,1,4,179
  Fri 01/18/2008 15:19:49.43

1 SSL VPN Client(s) installed
```

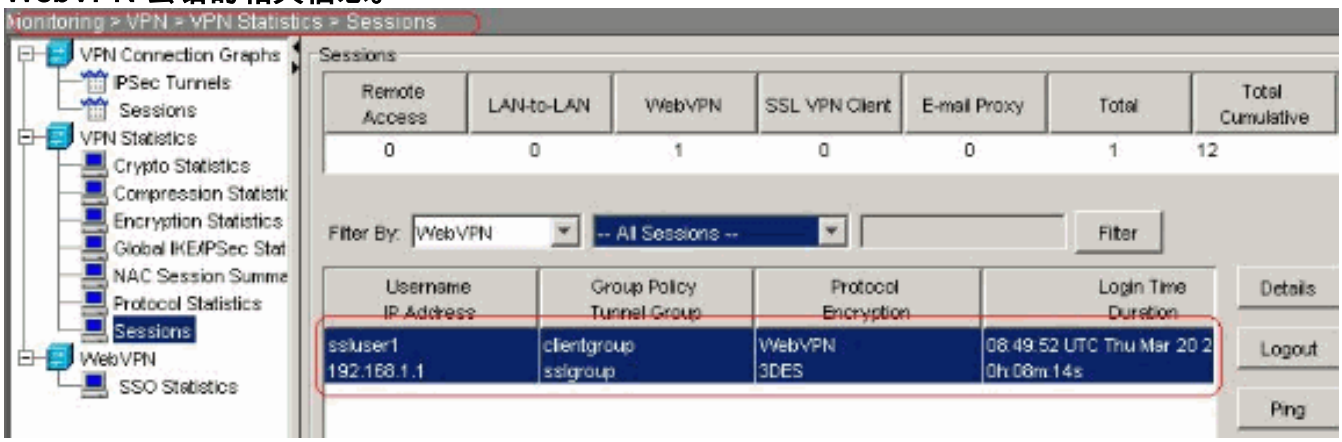
- **show vpn-sessiondb svc — 显示有关当前 SSL 连接的信息。**

```
ciscoasa#show vpn-sessiondb svc

Session Type: SVC

Username     : ssluser1
Index        : 1
Assigned IP  : 192.168.10.1           Public IP    : 192.168.1.1
Protocol     : SVC                    Encryption   : 3DES
Hashing      : SHA1
Bytes Tx     : 131813                 Bytes Rx     : 5082
Client Type  : Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
Client Ver   : Cisco Systems SSL VPN Client 1, 1, 4, 179
Group Policy : clientgroup
Tunnel Group : sslgroup
Login Time   : 12:38:47 UTC Mon Mar 17 2008
Duration     : 0h:00m:53s
Filter Name  :
```

- **show webvpn group-alias — 显示为各组配置的别名。**

```
ciscoasa#show webvpn group-alias
Tunnel Group: sslgroup   Group Alias: sslgroup_users enabled
```

- **在 ASDM 中，选择 Monitoring > VPN > VPN Statistics > Sessions 以了解 ASA 中当前 WebVPN 会话的相关信息。**



故障排除

本部分提供的信息可用于对配置进行故障排除。

1. **vpn-sessiondb logoff name <username> — 用于注销特定用户名的 SSL VPN 会话的命令。**

```
ciscoasa#vpn-sessiondb logoff name ssluser1
Called vpn_remove_uauIth: success!
webvpn_svc_np_tear_down: no ACL
```

```
NFO: Number of sessions with name "ssluser1" logged off : 1
```

同样地，您也可以使用 vpn-sessiondb logoff svc 命令终止所有 SVC 会话。

2. **注意**：如果PC进入待机或休眠模式，则SSL VPN连接可以终止。

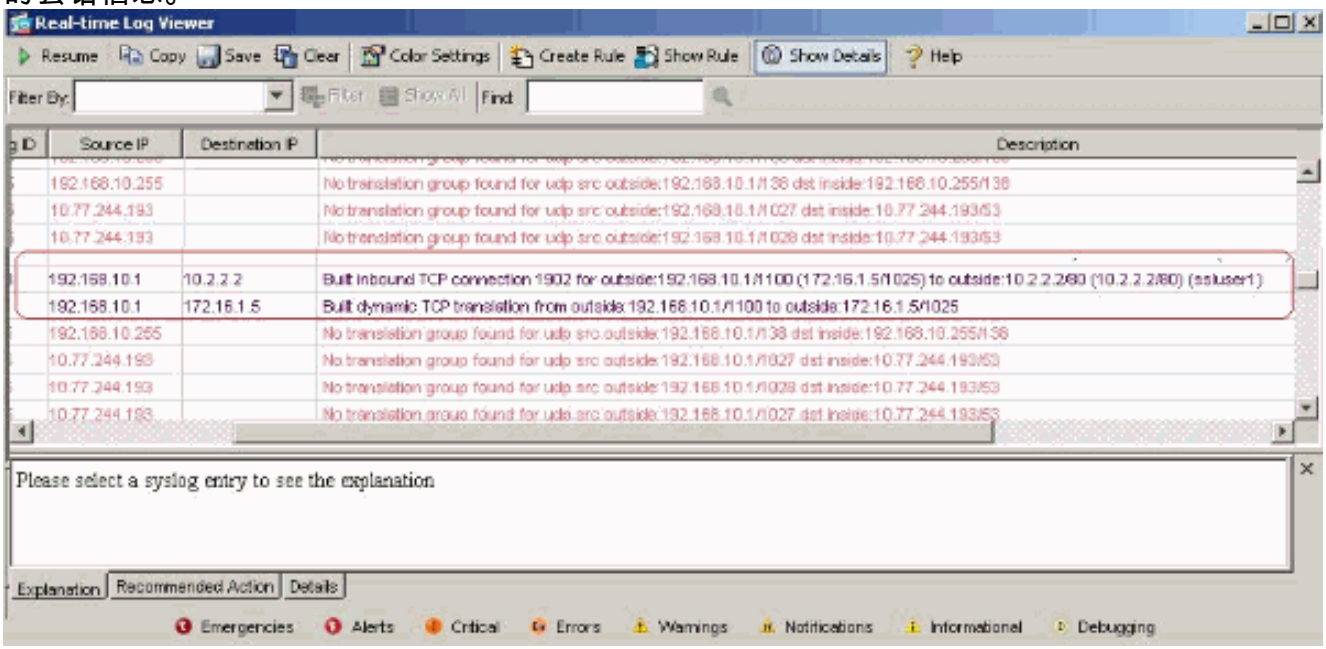
```
webvpn_rx_data_cstp
webvpn_rx_data_cstp: got message
SVC message: t/s=5/16: Client PC is going into suspend mode (Sleep, Hibernate, etc)
Called vpn_remove_uauth: success!
webvpn_svc_np_tear_down: no ACL



ciscoasa#show vpn-sessiondb svc
INFO: There are presently no active sessions
```

3. Debug webvpn svc <1-255> — 提供实时 webvpn 事件以建立会话。

```
Ciscoasa#debug webvpn svc 7

ATTR_CISCO_AV_PAIR: got SVC ACL: -1
webvpn_rx_data_tunnel_connect
CSTP state = HEADER_PROCESSING
http_parse_cstp_method()
...input: 'CONNECT /CSCOSSLC/tunnel HTTP/1.1'
webvpn_cstp_parse_request_field()
...input: 'Host: 172.16.1.1'
Processing CSTP header line: 'Host: 172.16.1.1'
webvpn_cstp_parse_request_field()
...input: 'User-Agent: Cisco Systems SSL VPN Client 1, 1, 4, 179'
Processing CSTP header line: 'User-Agent: Cisco Systems SSL VPN Client 1, 1, 4,
179'
Setting user-agent to: 'Cisco Systems SSL VPN Client 1, 1, 4, 179'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Version: 1'
Processing CSTP header line: 'X-CSTP-Version: 1'
Setting version to '1'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Hostname: tacweb'
Processing CSTP header line: 'X-CSTP-Hostname: tacweb'
Setting hostname to: 'tacweb'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Accept-Encoding: deflate;q=1.0'
Processing CSTP header line: 'X-CSTP-Accept-Encoding: deflate;q=1.0'
webvpn_cstp_parse_request_field()
...input: 'Cookie: webvpn=16885952@10@1205757506@D4886D33FBF1CF236DB5E8BE70B1486
D5BC554D2'
Processing CSTP header line: 'Cookie: webvpn=16885952@10@1205757506@D4886D33FBF1
CF236DB5E8BE70B1486D5BC554D2'
Found WebVPN cookie: 'webvpn=16885952@10@1205757506@D4886D33FBF1CF236DB5E8BE70B1
486D5BC554D2'
WebVPN Cookie: 'webvpn=16885952@10@1205757506@D4886D33FBF1CF236DB5E8BE70B1486D5B
C554D2'
Validating address: 0.0.0.0
CSTP state = WAIT_FOR_ADDRESS
webvpn_cstp_accept_address: 192.168.10.1/0.0.0.0
CSTP state = HAVE_ADDRESS
No subnetmask... must calculate it
SVC: NP setup
webvpn_svc_np_setup
SVC ACL Name: NULL
SVC ACL ID: -1
SVC ACL ID: -1
vpn_put_uauth success!
SVC: adding to sessmgmt
```

```
SVC: Sending response
CSTP state = CONNECTED
```

4. 在 ASDM 中，选择 **Monitoring > Logging > Real-time Log Viewer > View 以查看实时事件。**此示例显示 SVC 192.168.10.1 与 Internet 中 Webserver 10.2.2.2 之间通过 ASA 172.16.1.5 的会话信息。



相关信息

- Cisco 5500 系列自适应安全设备产品支持
- ASA/PIX：在 ASA 上允许 VPN Client 使用分割隧道的配置示例
- 路由器允许 VPN Client 使用分割隧道连接 IPsec 和 Internet 的配置示例
- PIX/ASA 7.x 以及用于公共 Internet VPN 的单接口 VPN Client 的配置示例
- 在 ASA 上用 ASDM 配置 SSL VPN Client (SVC) 的示例
- 技术支持和文档 - Cisco Systems